CPTE: Certified Penetration Testing Engineer

(5 Days)

***Includes exam voucher, course video, an exam preparation guide**

About this course

Certified Penetration Testing Engineer certification course is built firmly upon proven, hands-on, Penetration Testing methodologies utilized by our international group of vulnerability consultants.

The C)PTE presents information based on the 5 Key Elements of Pen Testing; Information Gathering, Scanning, Enumeration, Exploitation and Reporting. The latest vulnerabilities will be discovered using these tried and true techniques. This course also enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls to reduce risk associated to working with the internet. Besides utilizing ethical hacking methodologies, be prepared to learn penetration testing using advanced persistent threat techniques.

The C)PTE was developed around principles and behaviors used to combat malicious hackers and focuses on professional penetration testing rather than “ethical hacking”. With this in mind, the CPTE certification course is an up-grade to the EC-Council CEH!

Prerequisites

- A minimum of 12 months experience in networking technologies
- Sound knowledge of TCP/IP
- Knowledge of Microsoft packages
- Network+, Microsoft, Security+
- Basic Knowledge of Linux is essential

Target Student:

- Pen Testers
- Ethical Hackers
- Network Auditors
- Cyber Security Professionals
- Vulnerability Assessors
- Cyber Security

Course Objective

Upon completion, Certified Penetration Testing Engineer students will be able to establish industry acceptable auditing standards with current best practices and policies. Students will also be prepared to competently take the C)PTE exam.

Course Outline

Module 1: Business and Technical Logistics of Pen Testing
Lab – Getting Set Up

- Exercise 1 – Naming and subnet assignments
- Exercise 2 – Discovering your class share
- Exercise 3 – VM Image Preparation
- Exercise 4 – Discovering the Student Materials
- Exercise 5 – PDF Penetration Testing Methodology's review

Module 2: Linux Fundamentals
Lab – Linux Fundamentals

- Exercise 1 – ifconfig
- Exercise 2 – Mounting a USB Thumb Drive
- Exercise 3 – Mount a Windows partition
- Exercise 4 – VNC Server
- Exercise 5 – Preinstalled tools in BackTrack 5

Module 3: Information Gathering
Lab – Information Gathering

- Exercise 1 – Google Queries
- Exercise 2 – Footprinting Tools
- Exercise 3 – Getting everything you need with Maltego
- Exercise 4 – Using Firefox for Pen Testing
- Exercise 5 – Documentation of the assigned tasks

Module 4: Detecting Live Systems
Module 4 Lab – Detecting Live Systems

- Exercise 1 – Look@LAN
- Exercise 2 – Zenmap
- Exercise 3 – Zenmap in BackTrack 5
- Exercise 4 – NMAP Command Line
- Exercise 5 – Hping2
- Exercise 6 – Unicornscan
- Exercise 7 – Documentation of the assigned tasks

Module 5: Enumeration
Lab – Reconnaissance

- Exercise 1 – Banner Grabbing
- Exercise 2 – Zone Transfers
- Exercise 3 – SNMP Enumeration
- Exercise 4 – LDAP Enumeration

- Exercise 5 – Null Sessions
- Exercise 6 – SMB Enumeration
- Exercise 7 – SMTP Enumeration
- Exercise 8 – Documentation of the assigned tasks

Module 6: Vulnerability Assessments
Lab – Vulnerability Assessment

- Exercise 1 – Run Nessus for Windows
- Exercise 2 –Run Saint
- Exercise 3 – Documentation of the assigned tasks

Module 7: Malware Goes Undercover
Lab – Malware

- Exercise 1 – Netcat (Basics of Backdoor Tools)
- Exercise 2 – Exploiting and Pivoting our Attack
- Exercise 3 – Creating a Trojan
- Exercise 4 – Documentation of the assigned tasks

Module 8: Windows Hacking
Lab – Windows Hacking

- Exercise 1 – Cracking a Windows Password with Linux
- Exercise 2 – Cracking a Windows Password with Cain
- Exercise 3 – Covering your tracks via Audit Logs
- Exercise 4 – Alternate Data Streams
- Exercise 5 – Stegonagraphy
- Exercise 6 – Understanding Rootkits
- Exercise 7- Windows 7 Client Side Exploit (Browser)
- Exercise 8- Windows 2008 SMBv2 Exploit
- Exercise 9 – Documentation of the assigned tasks

Module 9: Hacking UNIX/Linux
Lab – Hacking UNIX/Linux

- Exercise 1 – Setup and Recon – Do you remember how?
- Exercise 2 – Making use of a poorly configured service
- Exercise 3 – Cracking a Linux password
- Exercise 4 – Creating a backdoor and covering our tracks
- Exercise 5 – Documentation of the assigned tasks

Module 10: Advanced Exploitation Techniques
Lab – Advanced Vulnerability and Exploitation Techniques

- Exercise 1 – Metasploit Command Line
- Exercise 2 – Metasploit Web Interface
- Exercise 3 – Exploit-DB.com
- Exercise 4 – Saint
- Exercise 5 – Documentation

Module 11: Pen Testing Wireless Networks
Lab – Attacking Wireless Networks

- Exercise 1 – War Driving Lab
- Exercise 2 – WEP Cracking Lab (classroom only)
- Exercise 3 – Documentation

Module 12: Networks, Sniffing and IDS
Lab – Networks, Sniffing and IDS

- Exercise 1 – Capture FTP Traffic
- Exercise 2 – ARP Cache Poisoning Basics
- Exercise 3 – ARP Cache Poisoning - RDP
- Exercise 4 – Documentation

Module 13: Injecting the Database
Lab – Database Hacking

- Exercise 1 – Hacme Bank – Login Bypass
- Exercise 2 – Hacme Bank – Verbose Table Modification
- Exercise 3 – Hacme Books – Denial of Service
- Exercise 4 – Hacme Books – Data Tampering
- Exercise 5 – Documentation of the assigned tasks

Module 14: Attacking Web Technologies
Lab – Hacking Web Applications

- Exercise 1 – Input Manipulation
- Exercise 2 – Shoveling a Shell
- Exercise 3 – Hacme Bank – Horizontal Privilege Escalation
- Exercise 4 – Hacme Bank – Vertical Privilege Escalation
- Exercise 5 – Hacme Bank – Cross Site Scripting
- Exercise 6 – Documentation of the assigned tasks

Module 15: Project Documentation

A5 Lab – Cryptography

- Exercise 1 – Caesar Encryption
- Exercise 2 – RC4 Encryption
- Exercise 3 – IPSec Deployment Post-Class Lab – CORE IMPACT
- Exercise 1 – CORE IMPACT